SPONGE ZINE #2

Assessing the Threats

Tech in Activism

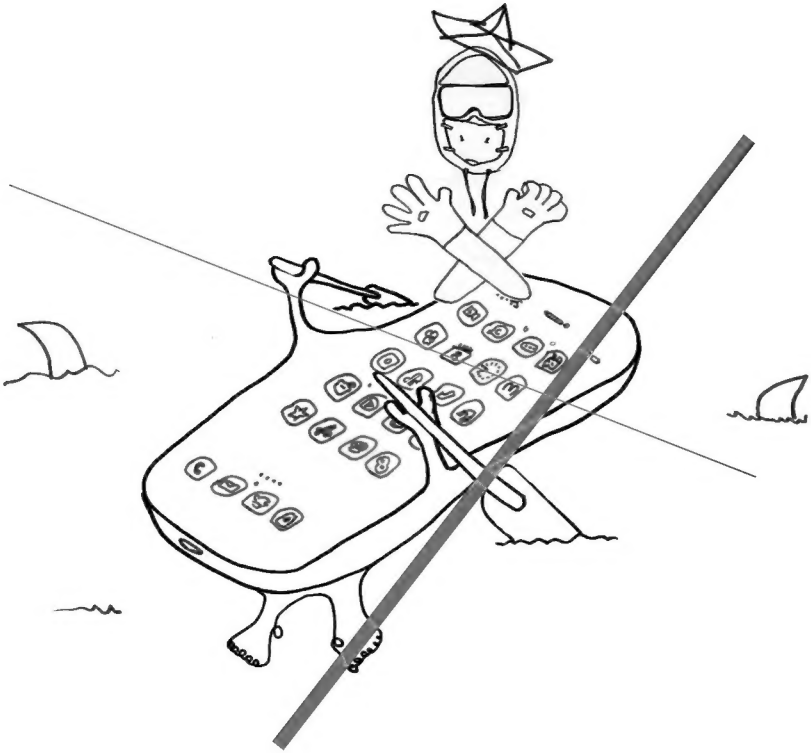
2026

DEMO
PHONE
03

03
WRITE
LAWYER'S
PHONE
NUMBER
HERE

Assessing the Threats Tech in Activism

2026



SPONGE ZINE #2

Plural Studio

Contents

Introduction

Section 01.

Self Awareness

An Integrated Approach to Living with Tech

Navigating Shifting Waters

Section 02.

Activist Networks

i. Assessing the Threats

ii. Building a Threat Model

iii. Appropriate Responses

Section 03.

Entering Public Space

i. Assessing the Threats

ii. Building a Threat Model

iii. Appropriate Responses

Updated and Available Yearly at the Plural Studio Linktree Here: https://tr.ee/V4GrqMeBfb

Index of Sections

Introduction

The core material that needs to be taken onboard in this zine is the following. 1. Make sure your mobile phone is capable of and does have full device encryption turned on when it is at rest - most new phones have this setting as default so simply check the sub section below on this topic to make use of it. 2. Update your software on all devices (further details below). 3. Use Signal messenger, and follow all the steps outlined in that section.

Be aware that an unaffected smartphone with radio signals turned off (i.e in Airplane Mode) and with the GPS deactivated (i.e, by turning Location Services or Location off), and with Bluetooth turned off, does not know where it is. A Faraday Pouch is not necessary.

Note that the advice in this guide is dated to June 1st, 2026 and that the advice here will need to be redrafted and updated after one year (around March 1st 2027), (outside of any potential and significant legal changes that could move a necessary guide advice update, forward). Companies' methods of tracking are constantly evolving as people figure out ways to avoid it. This advice could quickly fall out of date.

All living beings need boundaries. The greater their ability to sustain those boundaries, the greater the well-being of the living organism. Broadly, the boundaries that humans need to maintain often involve emotional, physical, social and legal points of entry and exchange. Sites of entry are potential sites of vulnerability. Vulnerabilities are found at the

locations of exchange that are necessary for life to go on. Vulnerabilities therefore exist as cultural, technical and environmental landscapes of maintenance. In the tech security language this perspective describes each unique situation as a “risk landscape”. The goal of this publication is to protect ourselves and one another. To raise awareness of potential threat scenarios/situations and encourage a culture of awareness that is prepared in advance to design and implement appropriate responses to such threats against activist networking, organizing and action.

Acting responsibly towards online threats is not simply an app I can purchase. Is not a new titanium door that I can order online. The logic of consuming our way out of danger is inherently flawed because it defeats at the outset the development of the new ways of thinking that will create flexible and situation appropriate thinking and action.

As activists we face certain kinds of threats that other citizens do not. Though the threats that any person faces by being online, networked and connected via technology are sufficient to raise awareness in themselves. It is rather that those systemic threats can be leveraged against activists later on. Complacency around tech masks the deeply bureaucratic and complex realities of networked technology creating barriers to engagement. This publication attempts to identify the measures needed to assess a given threat level for activists in the contexts outlined in each section. It is structured chronologically following a typical sequence of developing the intention to act, networking with more seasoned activists, organizing and participating in a public action such as direct action, and finally, addressing anything

that those threat scenarios may have overlooked due to information overload! More widely it is an attempt to de-normalise the surveillance and tracking that is inherent to using modern technology (whether the data is uploaded in real time or collected and transmitted later).

“Keeping good time is about knowing how to tell the time, even if you don’t own a real watch, and simultaneously about knowing whose time it is. In a phrase, keeping good time is about taking sides.”

- Avery F. Gordon

In the context of this publication keeping good time is also about maintaining our technological safety landscapes. It begins in section one with the maintenance of our personal space to support the creation of good work. Good work meaning ethical work done in a manner that ensures the maximum safety for those involved. Personal space meaning our interior emotional worlds and the bodies these worlds are housed within. As this publication is intended for activists and those who are fairly new to activism, a certain amount of ethical use is implied and expected of the reader. Such ethical presumptions however cannot be adopted when creating a threat model for any given situation. One must take a clear minded approach when modeling each scenario. As we see all around us, there are no rules in war, so one must assume that an adversary could indeed behave outside of one's imaginary.

"It is not enough to do the right things. We have to also do them for the right reasons, not just from an ethical perspective, but because the analytic tools that come from well-developed liberatory theories allow us to spot false allies and snitches easier."

- Popsec, Andor

https://opsec.riotmedicine.net/static/downloads/popsec-andor_a5.pdf

Ideally this publication will teach the reader to model and reason about data flows. To feel confident in reaching out and organizing with others and to apply appropriate responses to identified risks.

Section 01. Self Awareness - An Integrated Approach to Living with Tech

In order to combat the potential threats that technology poses to activists it is necessary to assess the possibility and probability of a particular event occurring. There are measures that individuals can take to lower the probability of phishing, doxxing or hate mail that work generally, but the responsible way to approach threat level awareness and risk assessment is to design your responses for each specific risk scenario. In any case, in this opening section the emphasis will be on the somewhat different impact digital technology has upon the human mind and body, other than security threats per se. An integrated approach to living with tech is about safe practices and staying informed in order to adapt

to new threat vectors. It is also about reclaiming our interior worlds. Centering the body in how we understand our relationships with the world is known as an integrated approach and borrows from the work of somatic body psychotherapists, activists in the digital sphere and others.

An analogy between surfing or sailing with digital technology has extended the physical object of the smartphone to grow our boundaries for decades. In this section I will use the analogy of sailing amongst waves of data as a way to understand, set and maintain those boundaries. A human rides the waves wearing a boat that needs constant maintenance to keep the water out. Let's begin with some exercises to ground the reader in their body, in the present moment. The goal of this section is to advance the experiences we have of our inner worlds so that we might be able to return to this grounded space in order to respond more effectively to high stress situations later.

To begin with - where is your phone right now? How has it shaped your clothing over the years? Your body posture as you use it? How has using this piece of tech created muscle memories that are now stored at different locations within your body? Let's deactivate your mobile supercomputer smartphone for this first section, as a way to look at the technology we are immersed within, from a new perspective. The device could be put on silent, Airplane mode, in another room, turned off and/or stashed in a Faraday blocking pouch. Whichever you feel comfortable with. Now that you are feeling comfortable and relaxed, consider the vast network of your muscles, nerves, veins and arteries working tirelessly day and night. Take a deep breath and let each aspect of

your body relax, area by area, system by system.
Close your eyes if this helps.

“Get comfortable and take a few deep breaths. Let your shoulders relax. Place your palm on the center of your belly, just above your navel. Press in gently. Hold your hand in place for a moment or two. Then, slowly rub your belly for three to four minutes, in whatever way feels good to your body. When you're done, pay attention to all the sensations in your body. You can do this with or without clothes, but remove any heavy outerwear.” - Resmaa Manakem - My Grandmother’s Hands

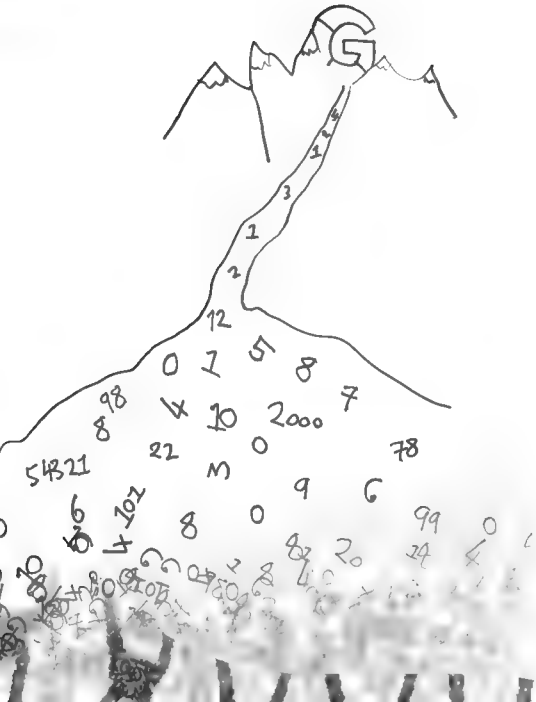
Alternatively count your breathing in a timed cycle. This creates deep bodily calm. Inhale for a number of counts that feels comfortable, hold the breath for the same number then breath out for an equal count and wait to breathe in again for the same amount again. Try this for two minutes when things get hectic. Ideally just beforehand.

As a general form of maintenance, make sure your physical health advances parallel to your mental and digital well-being. Conceive of them together and try not to get into a habit of trading one for the other. The body is where the mind happens. A temperate and healthy activist can achieve more and help others up and into greater well-being as they go. You may want to follow Taoist principles of energy conservation. Or to follow the Buddhist goal of *treating that which has weight with lightness and that which is light with weight*. It is also good advice to look up Tactical Tech's book, Holistic Security.

The Boats We Wear

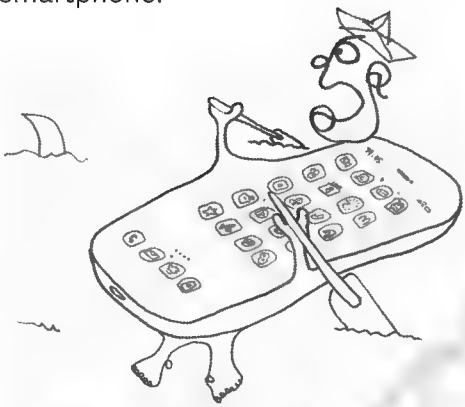
Arguably, humans tend to think of our digital technology as something we consume and use privately. The opposite is closer to the truth: our tech is more like clothing that we wear: it displays our lives to anyone who wants to know and is resourced to find out - hackers, governments, advertising agencies, political think tanks... Or followers on social media accounts!

At first it was just a stream of data, trickling down a proverbial hillside....



That innocent stream soon became a torrent. And vast oceans of data began to pool and connect, seeping further and further into our lives.

In response to the availability of new technologies, if you like, humans built boats, most commonly in the form of the smartphone.



Smartphones, however, only allow us to move about in the sea of data, and create digital footprints of location data as we go. We are most consumed by data surveillance when we sail into it on our smartphones. But in terms of broken boundaries, centralized data stores and services, undersea cables, and large network switches are the largest sites of data leaks.

The covid lockdowns certainly moved the human further online, multiplying the points of entry and exchange where vulnerabilities can occur, in parallel to the establishment of a truly global online network where social space is reproduced. Fact is, in the modern world - we sail. So how can I, an individual, prevent my boat from leaking data out into the ocean, or letting a sea of malware, phishing scams and who knows who - in?

The analogy between sailing and surfing the web is not perfect. But I hope it conveys a sense of scale and provides an imaginary to work with. Lighthouses in the distance, flotillas of connected devices traveling together to discover new things about their local environments. Learning to read your body's responses to a situation will help you to make good decisions under pressure. Keep in mind that boats are subject to entropy: like everything else they wear down. Maintaining the security updates of the device you sail in, is like tending to a garden. As time goes on it is the organisms that adapt that survive.

Does your device tell you when you need to update? How do you respond? Sometimes pushing "update later" for two weeks is enough for a breach of your device. To understand why it is so crucial to maintain updates see the section below on PDF's and malware that exploits known weaknesses in software, like Word or Excel.

If a Mac passes the date where it can continue to have the browser securely updated, it can be re-fitted with Xubuntu or other software. This also applies to other computer models/ companies. One issue to look out for here is the permanent firmware within a computer that cannot be replaced, and which may yet have unknown vulnerabilities.

Digital security is a state of mind, not a finish line. Like all forms of security within conflict situations, the quality of the threat model created for each scenario will determine the success and potential prevented losses associated with that activity. And while this guide is far from complete it should open up an awareness as to what lurks beneath the

electronic currents that shape and are shaped by living heartbeats. In the long run we may find that the measures outlined here are as crucial to the social body as safe sex, driving on the right side of the road and protecting the vulnerable from harm - for everyone. As activists they are crucial to organizing in the 21st century. The corporate governance model of liberal democracy has not worked to save lives and prevent harm. It is up to us find ways to have conversations about assessing the threat level with and within the groups we make kin. Against all the odds, we have to make this work.

If reading this guide stimulates your freeze, fight or flight (vagus nerve) system, this is a natural human response. There is no shame in what your body is telling you. Stay with the body as you go forward and take the guidance compiled here one day, one week, or even one month at a time.

Staying with the body means noticing how your body responds to the events and relationships in your life. Humans are social animals and being with others might sometimes require a leap of faith. Healing happens with others in whichever format is available to you. That might mean joining a group, it might mean having a good cry in private. Crying at the state of the world is also completely normal and natural. After all, as a wise wom*n once said:

‘Water is emotion, breaking into consciousness.’

- Janine Mather

Navigating Shifting Waters

Different digital service providers and platforms have different political approaches towards the ownership of the data they receive and process.

They range from completely de-centralized, non-hierarchical collectives at one end of the spectrum, to monopolistic tech corporations at the other.

A corporate digital monopoly treats the user as a product (which is why their services are “free”). Any data point about you that can be (in principle) legally identified, captured and stored during your interaction with that platform or service can and will be accumulated for further use/sale.
In the middle of the these two different attitudes to the digital lives of other human beings are non-profits that see themselves as contributing to the common good, and private companies that simply engage in different forms of the capitalistic free market. The spectrum above demonstrates a political climate also: the more Left Wing platforms privilege humans over markets, and vice versa for those on the Right.

For this edition of the Sponge Zine we have

developed a way of grading threat scenarios across this spectrum of possible digital platforms. The grading system allows these interactions to be visualized.

We tried to tie the political climate of each platform or service to different weather patterns that the user should prepare for. The reader should be able to use this system to foresee the effects of the political climate associated with the digital services they will encounter while carrying out their activity.

The system is expanded on the following pages. The goal is that each reader is ultimately able to develop their own personal shipping forecast that can be applied to their use of digital technologies.

We have also applied this grading system, with diagrams and reminders, to each section of the guide as it can take a minute to digest.

You may ask 'where is the political state in all this?' and it is sobering to acknowledge how intertwined Big Tech has become with traditional state apparatus such as healthcare, the military, education, the economy and policing to name but

the most obvious arenas. While the corporate takeover of all nation states is not yet complete and much more could be said on this complex dynamic, it is worth remembering that from a safety perspective the oceans of Big Tech are more than well equipped to hand over highly detailed information about individuals targeted by authorities. The naked ambition of Big Tech is a clear and present danger which is why pushback, for example in the EU has become a primary battle line for human rights and the rule if law going forward.

a spectrum of possibilities

big tech ocean:
publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need:
FACE MASK, GLOVES and GOGGLES

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take:
UMBRELLA

possible

dig

for digital platforms

non-profit lake:
(signal, firefox, etc)

LIGHT SHOWERS

user vigilance should ensure protection from leaks or boat breach

Go for a:
SHOWER PROOF JACKET

pond of autonomous tech infra:
riseup, autistici/ inventati, systemli, etc

MISTY

data is minimized as a principle, identities remain anonymous

Wear a:
PAPER BOAT

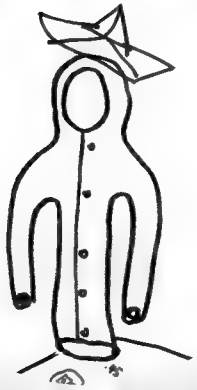
gital platforms

pond of autonomo-us tech: MISTY

Think about what you post and where you conduct conversations on social media. Each interaction creates a permanent record. Some spaces and places on the web use a more autonomous tech to create an atmosphere of trust, for exampe anonymous hosting of projects that align with a group's values.

Digital security cultures share common languages, like all cultures. Ideally, people using autonomous tech infrastructure will respect your privacy, your express wish for anonymity and your personal boundaries. The paper boat hat or other sign/avatar or symbol in the user's personal bio indicates that they will actively maintain the boundaries of the autonomous network and report violations of the code of conduct.

non-profit lake: LIGHT SHOWERS



For example – using a VPN to mask your IP address will enhance your privacy, like choosing an anonymous avatar on social media. However, neither of these precautions will prevent the vast majority of identifying correlations that reveal your credentials.

Like most measures intended to enhance personal data privacy, the threat assessment involved here creates individually oriented outcomes that are more isolated and therefore thinner as protective boundaries.

private company river: CONDITIONS UNCERTAIN

Be discreet when sharing your Signal contact by only sharing the Signal handle and not your phone number and maintain your anonymity by using a pseudonym during activist networking.

Private companies permeate the data-sphere and it is impossible to know if someone you meet at an event is conducting the same threat assessments or what kind of digital infrastructure you will be encouraged to sail through in order to attend it. Perhaps the event has a sign-up registration portal online. Or the given sailing route could demand that you download an unsecure travel app in order to get there. You may barely notice the data points collecting around you until the wind changes in the future and issues a jet of water in the face.

ocean of big tech: ROUGH WEATHER

If you anticipate ROUGH WEATHER turn Flight Mode: ON, turn Phone Location Services: OFF. Turn Bluetooth OFF. Do this at home, before entering the rough weather of public space.

Let's say you attend a protest or seek to otherwise intervene in the status quo through direct action. This would be ROUGH WEATHER involving: state video and data collection surveillance, for example, phone number tracking and association with biometric information, your address etc, possible phone seizure and infiltration (upon potential arrest), images being captured of you and posted to social media with metadata still attached, all of which will likely be made available to the LLM's of the given corporate-state actors currently in possession of the contracts to that data.

Section 02. Activist Networks

i. Assessing the Threats

Activists network in order to bring about improvements to the wellbeing of humans, other living organisms and the wider environment on which all life depends. This work often involves fending off threats from aggressors. The use case for this section is designed for those who are relatively new to activism or those who wish to use this guide to explain to new members of an intentional activist community how to practice a basic level of security. Networking creates the crucial points of entry and exchange that can also lead to vulnerabilities. It is therefore here that specific care must be taken when engaging and exchanging with others.

Communication and social contact is heavily facilitated by tech in the modern world. The primary activity of networking is to make contacts and stay in touch. The following advice is designed to respond to the threat of activists having their true identity revealed in connection with their activism, targeted attacks (often much later than the point of initial contact) to extract data (for example via malware), infiltration of working groups by an aggressor to extract and collate data, and/or historical message records being access by authorities if technology is confiscated upon arrest. [Note that the above list covers cases where data is stored locally, but the use of services like traditional social media or even most email, means that there are two additional ways that governments/corporations get data: by collecting data in bulk as it moves (mass surveillance) or by requesting it later from corporate servers (legal requests). One way to build a "threat model" is to think about each of these types of threats and their timing, which ones are most problematic for you, and

what to do to prevent each.]

ii. Building a Threat Model

Because it is difficult to gauge the true intentions of the new people that one might meet, it must be assumed that in the context of an activist networking event no-one should be given access to unnecessary private information, full name or (non-temporary) contact details. It is important to maintain this stance for the safety of all despite perhaps recognizing some of the colleagues in attendance. The goal is to encourage and practice a culture of security. Note that such meeting spaces are not safe places to discuss potential actions. If someone feels uncomfortable with a completely new face that no-one can vouch for at the meeting that person should be able to be asked to leave and to understand why this is appropriate. It will not be appropriate to discuss the presence of persons and conversations held within the space of the meeting thereafter, depending on the content and context of the meeting. Again, assessing the threats will provide the appropriate security measures. Don't burden friends and family with gossipy details about potential activity they do not need to know as a rule of thumb.

iii. Appropriate Responses

Although you, the reader possibly did not turn off or stash their smartphone away in section one, if you did then let's now fire that baby up and patch some potential holes in the boats we wear. The next big must for all modern data-faring craft are those pesky security updates. If your device can no-longer support updates it might be time to use it for something else other than being connected to the internet.

Hard Borders
Here is the current advice from Electronic Frontier Foundation:
A Journalist Security Checklist: Preparing Devices for Travel Through a US Border

https://www.eff.org/deeplinks/2025/06/journalist-security-checklist-preparing-devices-travel-through-us-border

Your border digital security checklist:

Preparing for travel
☐ Make a backup of each of your devices before traveling.
☐ Use long, unpredictable, alphanumeric passcodes for your devices and commit those passwords to memory.
☐ If bringing a laptop, ensure it is encrypted using BitLocker for Windows, or FileVault for macOS. Chromebooks are encrypted by default. A password-protected laptop screen lock is usually insufficient. When going through security, devices should be turned all the way off.
☐ Fully update your device and apps.
☐ Optional: Use a password manager to help create and store randomized passcodes. 1Password users can create temporary travel vaults.
☐ Bring as few sensitive devices as possible — only what you need.

big tech ocean:
publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**

☐ Regardless which country you are visiting, think carefully about what you are willing to post publicly on social media about that country to avoid scrutiny.
☐ For land ports of entry in the U.S., check CBP's border wait times and plan accordingly.
☐ If possible, print out any travel documents in advance to avoid the necessity to unlock your phone during boarding, including boarding passes for your departure and return, rental car information, and any information about your itinerary that you would like to have on hand if questioned (e.g., hotel bookings, visa paperwork, employment

information if applicable, conference information). Use a printer you trust at home or at the office, just in case.
☐ Avoid bringing sensitive physical documents you wouldn't want searched. If you need them, consider digitizing them (e.g., by taking a photo) and storing them remotely on a cloud service or backup device.

Decide in advance whether you will unlock your device or provide the passcode for a search. Your overall likelihood of experiencing a device search is low (e.g., less than .01% of international travelers are selected), but depending on what information you carry, the impact of a search may be quite high. If you plan to unlock your device for a search or provide the passcode, ensure your devices are prepared:
☐ Upload any information you would like to keep in cloud providers in advance (e.g., using iCloud) that you would like stored remotely, instead of locally on your device.
☐ Remove any apps, files, chat histories, browsing histories, and sensitive contacts you would not want exposed during a search.

☐ If you delete photos or files, delete them a second time in the “Recently Deleted” or “Trash” sections of your Files and Photos apps.
☐ Remove messages from the device that you believe would draw unwanted scrutiny. Remove yourself — even if temporarily — from chat groups on platforms like Signal.
☐ If you use Signal and plan to keep it on your device, use disappearing messages to minimize how much information you keep within the app.
☐ Optional: Bring a travel device instead of your usual device. Ensure it is populated with the apps you need while traveling, as well as login credentials (e.g., stored in a password manager), and necessary files. If you do this, ensure your trusted contacts know how to reach you on this device.
☐ Optional: Rather than manually removing all sensitive files from your computer, if you are primarily accessing web services during your travels, a Chromebook may be an affordable alternative to your regular computer.
☐ Optional: After backing up your devices for every day use, factory reset it and add only the information you need back onto the device.
☐ Optional: If you intend to work during your travel, plan in advance with a colleague who can remotely assist you in accessing and/or rotating necessary credentials.
☐ If you don’t plan to work, consider discussing with your IT department whether temporarily suspending your work accounts could mitigate risks at border crossings.

On the day of travel
☐ Log out of accounts you do not want accessible to border officials. Note that border officers do not have authority to

access live cloud content — they must put devices in airplane mode or otherwise disconnect them from the internet.

☐ Power down your phone and laptop entirely before going through security. This will enable disk encryption, and make it harder for someone to analyze your device.

☐ Immediately before travel, if you have a practicing attorney who has expertise in immigration and border issues, particularly related to members of the media, make sure you have their contact information written down before visiting.

☐ Immediately before travel, ensure that a friend, relative, or colleague is aware of your whereabouts when passing through a port of entry, and provide them with an update as soon as possible afterward.

If you are pulled into secondary screening

☐ Be polite and try not to emotionally escalate the situation.

☐ Do not lie to border officials, but don't offer any information they do not explicitly request.

☐ Politely request officers' names and badge numbers.

☐ If you choose to unlock your device, rather than telling border officials your passcode, ask to type it in yourself.

☐ Ask to be present for a search of your device. But note officers are likely to take your device out of your line of sight.

☐ You may decline the request to search your device, but this may result in your device being seized and held for days, weeks, or months. If you are not a U.S. citizen, refusal to comply with a search request may lead to denial of entry, or scrutiny of lawful permanent resident status.

☐ If your device is seized, ask for a custody receipt (Form 6051D). This should also list the name and contact information for a supervising officer.

IF THEIR ABSENCE BRINGS YOU PEACE,
YOU DIDN'T LOSE THEM.
AGING IS AN EXTRAORDINARY PROCESS
WHERE YOU BECOME THE PERSON YOU ALWAYS SHOULD HAVE BEEN.
OF COURSE I STRUGGLE.
I ALSO DON'T FUCKING QUIT.
EVERYONE WHO'S INTERESTING REINVENTED THEMSELVES AFTER THEIR WORLD FELL APART.
JUST LIKE YOU DID.
NOTHING IS NORMAL AND NO ONE IS OKAY.
YOU'RE DOING GREAT.

YOU CAN FORGIVE SOME PEOPLE WITHOUT WELCOMING THEM BACK INTO YOUR LIFE.

APOLOGY ACCEPTED, ACCESS DENIED.

BEING AT EASE WITH NOT KNOWING

IS CRUCIAL FOR ANSWERS TO COME TO YOU.

BE CAREFUL WHAT YOU TOLERATE.

YOU ARE TEACHING PEOPLE HOW TO TREAT YOU.

IF STANDING UP FOR YOURSELF BURNS A BRIDGE,

FUCK THAT BRIDGE.

BE MESSY, COMPLICATED, AND AFRAID

AND SHOW UP ANYWAY.

Inspirational Skeletor
@skeletor@mas.to

☐ If an officer has plugged your unlocked phone or computer into another electronic device, they may have obtained a forensic copy of your device. You will want to remember anything you can about this event if it happens.
☐ Immediately afterward, write down as many details as you can about the encounter: e.g., names, badge numbers, descriptions of equipment that may have been used to analyze the device, changes to the device or corrupted data, etc.

Reporting is not a crime. Be confident knowing you haven't done anything wrong. - Electric Frontier Foundation

Finally, consider factory reset before travel through particularly risky borders. If you cannot take any of the above measures, and decide to simply delete the Signal application or similar, also purge the data/cache associated with the application, understanding that unless you back up the chats, you will lose most of them and this could impede your efficacy as an activist.

* * *

Signal
@signalapp@mastodon.world
Apr 27

For the time being, please stay vigilant against phishing and account takeover attempts. Remember that no one from Signal Support will ever send you a message request or ask for your registration verification code or Signal PIN. For an added layer of protection, you can enable Registration Lock in your Signal Settings (Account -> Registration Lock). 8/

Using Signal

The messaging app Signal is the most commonly used safer communication system.

This section references: Electronic Frontier Foundation (EFF); CAIR SFBA Digital Security Handout "Digital Security 101" b44:34. @18millionrising; Zebra Crossing Digital Safety Checklist; Freedom of the Press Foundation "Digital Security Guides"; Access Now Digital Security Helpline; Equality Labs' "Anti-Doxing Guide for Activists")

non-profit lake:
(signal, firefox, etc)

LIGHT SHOWERS

user vigilance should ensure protection from leaks or boat breach

Go for a:
SHOWER PROOF JACKET

1. Fix Your Notifications: In Settings › Privacy or Notifications or both, make sure that notifications ONLY include the fact that a message arrived in Signal - NOT name of sender or message contents. Otherwise this data can be subpoenaed from Google or Apple. This is exactly what occurred in the Texas trial against multiple Antifa activists in 2026 when the FBI was able to forensically extract copies of incoming Signal messages from a defendant's iPhone. This was possible even after the app had been deleted, because copies of the content were saved in the device's push notification database, as reported by 404 Media.

2. It is crucial to keep Signal updated. If you don't - as with any application - you are putting people at risk, for example by exposing their phone numbers if your device is seized, or by leaving it vulnerable to hacking. Search for the

application in your app store and click update.

3. Create a Username via: [Settings › Your own profile at top › Add a username] Choose something you are not attached to and feel comfortable changing if necessary. Note: Your Username is not your Display name. Changing your Display name won't help protect you much as the name change shows up in all the chats you're in. Moreover, frequent Display Name changes will make it more difficult for comrades and group admins to know who is in the group and detect infiltrators.

4. Set Up Default Disappearing Messages: [Settings › Privacy › Disappearing Messages] Set up a reasonable time globally (1 day/8hrs/1 week) but extra short if you are dealing with sensitive information or discussing on-the-ground activity. This will need to be longer or shorter depending on the content of your conversations/action, but it is important that it be something that is not forever. Note that this is only a default for new chats that you start. If someone writes you, or adds you to an existing group, it is your responsibility to adjust the disappearing message time appropriately and avoid activist chats having messages retained forever - who knows who will go through a border crossing or get infected with malware in a few months or years! If you have already started conversations with activists, delete any unnecessary messages you already have, and turn on disappearing messages.

5. Hide Your Phone Number: [Settings > Privacy › Phone Number] The first of the two option dialogs MUST be set to "Nobody". Do Not Give or Request Phone Numbers to Make

Contact on Signal. When meeting people, provide the username or QR code, NOT your phone number. Ideally, try to remember your username so you can give it in places where you do not want to be on cellular network. Do not add activists' emails or phone numbers to your phone's "Contacts" if you only intend to communicate on Signal.

6. Finally, when meeting people, provide the username, NOT your phone number, to avoid them adding it to contacts or calling/SMSing it over the public switch telephone network. To do this go to the pencil icon at the top right of your list of conversations - not the large search bar below or above. Add the persons' username or click “Accept” if they have contacted you. Remember to set disappearing messages before starting a conversation.

7. Change your username (such as Lex.1312) periodically but do not change your display name (the one other people see in the chat), too often. It makes it harder for activist groups to know they're familiar with the members, to detect infiltrators. The point of changing a username is so that a cop doesn't try to impersonate a friend.

8. Heads up from a data security colleague: Apple Intelligence can now read Signal messages on iPhones. If you have iOS 18.1 or higher, disable Apple Artificial Intelligence under settings, or go under Siri/AI and ensure it is not enabled for Signal. If you do not, it can scan your Signal messages and read the content. To do so, navigate to Settings › Siri › scroll down to Apps › Signal › turn off "Learn from this app" and the other two or three settings.

Not Using Telegram

Do not use Telegram for activism in any way. Telegram creates the impression that it is safe but is not end to end encrypted and therefore unsafe. It's also unaccountable as their code is not transparent. Handing y/our metadata - records of the sender, receiver and time of the message to Telegram's servers to be stored there indefinitely is the same as posting your content to other private companies that run social media platforms and regularly hand user data over to authorities, the same is true for proton email to some degree. They communicate in a way that creates a false sense of security amongst their users. IF YOU USE TELEGRAM or Instagram be sure to take your messages/conversations to Signal as soon as possible, having hidden both your phone numbers.

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**

Email

Mailbox.org and Posteo are paid email providers, although Protonmail has a free tier. Protonmail is encrypted (for now) in a way where the provider's servers do not store readable copies of your stored emails. Email should be avoided for

activism that intelligence services might be interested in, because some of them can read emails as they're being sent between different providers. Emails sent between Protonmail accounts are somewhat safer, though proof of account ownership from bank transfer records can be subpoenaed by authorities. Use a strong password. Emails are still necessary and useful for some purposes sometimes in activism, for example not for sending messages about actions or planning, but as a way to sign up for or log into accounts on other services, as a backup method of communication with a clear intent about when to use them and when not (mostly not) or to be on mailing lists or interact with larger official organizations. In these cases the reason we recommend Protonmail and Posteo paid tiers if you can afford them is because they allow you (together with simplelogin.com which comes with the Protonmail paid service) to generate lots of different identities, making it much harder for private companies, and a bit harder for governments, to map out the structures of social movements, figure out your identity, or target you or your accounts for compromise.

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**

Apps

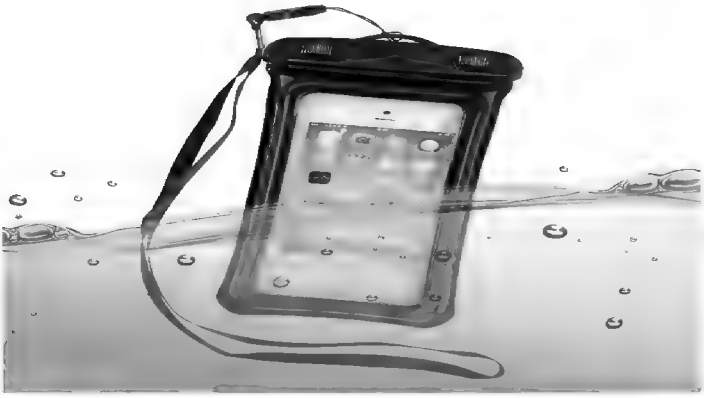
Having fewer apps is better; each app has its own potential security failures or exploits (or active data collection about you!). Instead of installing new apps for every service, consider if you can use a website in your browser. Some websites insist that you install an app, but sometimes if you go to the menu or settings and choose "See desktop version" it works as a website without requiring you to install an app! For the apps you do have, including browsers (where Firefox, Brave and Chrome without Google login are a better choice than Safari), keep up with all software updates—these often address known security vulnerabilities.

big tech ocean: publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**



Not Sharing PDFs

Do Not Share PDFs and Office documents - A PDF document or Office document is so commonplace it is very easy to forget that they can include malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Screen shot the document and share those image files. If you are sharing images via the messaging app Signal, Signal will remove the image's metadata. This is not currently the case for video content. Other than images and video and audio and txt files sent through signal, do not open any attachments that you weren't specifically expecting to receive from someone, ever, unless a clear reason is given by your contact whom you know well and has good digital security practices - through a different means of communication than the one where the file came. For example, if you receive a file by email, write the friend on Signal [to ask about the attachment]. If you received it by signal, give the friend a call on Signal, or write them on Whatsapp or email. Even if you are told why it was necessary, see if there's another way to communicate the information.

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**

If you absolutely need to open PDFs more safely, the software Dangerzone is recommended. - https://dangerzone.rocks/about/

PDFs and office documents are incredibly complex. They can be made to automatically load an image from a remote server when the document is open, tracking when a document is opened and from what IP address. They can contain JavaScript or macros that, depending on how your software is configured, could automatically execute code when opened, potentially taking over your computer. And finally, like all software, the programs you use to open documents – Preview, Adobe Reader, Microsoft Word, LibreOffice, etc. – have bugs, and these bugs can sometimes be exploited to take over your computer.

You can reduce your risk of getting hacked by always installing your updates, which fix the bugs that software vendors are aware of. However, it is still important to avoid downloading attachments or files from unknown domain names - the first part of web addresses - the URL that you can read in the seqrch bar - after the slashes in https:// or http:// buy before the first slash of the URL - even if you have recent updates. Often governments know about vulnerabilities that the software companies don't yet.

For example, if an attacker knows about a security bug in Microsoft Word, they can carefully craft a Word document that, when opened using a vulnerable version of Word, will hack your computer. All they have to do is trick you into opening it, perhaps by sending you a convincing enough phishing email.

Tracking & Social Network Mapping

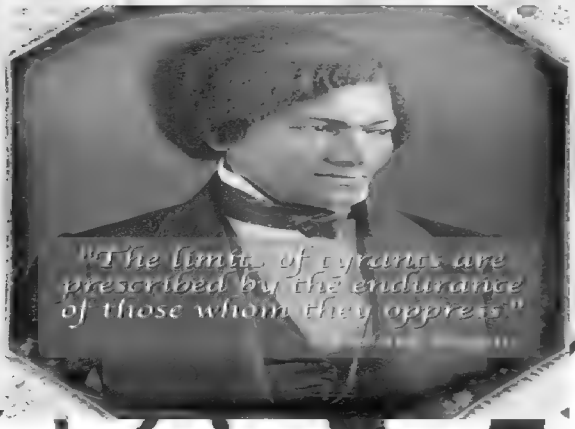
Tracking Metadata Data flows both into and out of our smartphones and computers constantly. Some of it is used to create a picture of us as we move around the web. For example all the language after the "?" in a link to the social media platform Instagram are tracking parameters, used for tracking the user and anyone they share that link with. However for many websites this is not the case and identifying and removing tracking parameters from URLs is highly complicated. For example the portion of a YouTube URL after the “?” And after v= and before the next & or end of the URL is the video ID, necessary for retrieving the video. Companies' methods of tracking are constantly evolving as people figure out ways to avoid it. This advice could quickly fall out of date.

big tech ocean: publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**



Section 03. Entering Public Space

What constitutes public space? The very idea of public space is somewhat fluid and difficult to generalize. For some it is simply a game where the appearance of striving for the common good is used to create specific social and economic outcomes. For others it is the very foundation of the democratic process and these definitions are not mutually exclusive. In so far as it legally or historically belongs to the public, (public) space is the place to articulate demands and shape our world. As such it will always be contested. One must also recognize that from the very beginning of this publication the digital space referred to as the sea of data is a form of public space. Only, like the city, with certain areas blocked off and privatised. The goal of this section is to provide advice for activists formally entering the public realm, be this 'in real life' or online (as opposed to meeting and organizing in private). Because at this point the probability of your full legal name, biometric data (such as a photograph of your face or your fingerprint), and personal information becoming known is much higher.

i. Assessing the Threats

As painful as it may be to think about, we should now develop a culture of security around the technological devices that have also brought us so many great things. Like this publication! Not only to disrupt surveillance capitalism and protect friends today, but in anticipation of a potential flood in which words could be taken out of context and weaponised later. It is worth noting that the advice in this section is good advice that could be meaningfully included within each of the previous ones, but that due to concerns

around the volume and delivery of information, this publication has attempted to break the core material it contains into chronological stages of awareness and active activist activity.

ii. Building a Threat Model

One has to anticipate that authorities will target and arrest activists in the public realm, even on peaceful and permitted public demonstrations. They will use their monopoly on violence which extends into raiding homes and searching all the confiscated tech available to them. In Berlin specifically, this activity is now legal for the police to carry out in secret, without informing the occupant. Authorities are also able to film within your home and install spyware on your devices as of January 2026, in Berlin, Germany. The threat is therefore related to information pertaining to activist activities, personal details, chat records and histories, shared files, photographs of colleagues etcetera. It may also be the case that by virtue of being in the wrong place at the right time guilt by association is leveled against activists.

As reported by 404 Media in 2024, a whistleblower leak strongly implies that large companies such as Facebook, Google and Amazon gather recorded audio from user's smartphones that is then used to profile them/us and more precisely target content, such as advertising. The leak states that Cox Media Group offer a service called Active Listening which records any audio available near enough to a smartphone to be captured.
https://www.404media.co/heres-the-pitch-deck-for-active-listening-ad-targeting/ That link has a paywall, so here is a less than precise summary from Dazed magazine. https://

www.dazeddigital.com/life-culture/article/64513/1/conspiracy-confirmed-phones-listening-everything-cox-media-cmg-facebook-amazon

And here are articles from techdirt https://www.techdirt.com/2024/08/29/cox-caught-again-bragging-it-spies-on-users-with-embedded-device-microphones-to-sell-ads/, Variety https://variety.com/2023/digital/news/active-listening-marketers-smartphones-ad-targeting-cox-media-group-1235841007/ and an archived copy of the original marketing pitch from CMG https://web.archive.org/web/20231214235444/https://www.cmglocalsolutions.com/blog/active-listening-an-overview

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**

iii. Appropriate Responses

Active Listening

Bear in mind that Apple's Siri, Google's Assistant and Amazon's Alexa already use a form of active listening as their main feature as a product. Have a look at see how many Apps on your phone Siri has access to, and adjust accordingly as outlined in section 8 of the section on Signal: navigate to Settings › Siri › scroll down to Apps › Signal › turn

off "Learn from this app" and the other two or three settings. If you determine that the threat level is high there are options for muffling your smartphone's microphone.

The advanced protection program for iOS is to switch on Lockdown Mode. It is also possible to remove a mobile supercomputer smartphone's internal speaker and use the device's Bluetooth to record, send and listen to audio.

According to a February 2026 article on Medium: Our Devices Are Listening to Us, by writer and technologist Giraldo Rosales, ambiguity around this threat is exactly the point: "Operating systems don't grant "partial listening" or "intent-only access." They grant access to hardware. What an app does with that access — whether it records full clips, samples short fragments, analyzes sound patterns, converts audio into metadata, or processes and discards signals immediately — is a design choice, not a technical limitation.

This is why companies are extremely careful with language. You'll hear phrases like "we don't record conversations for ads" or "we don't listen to private conversations." Those statements are narrow by design. They don't rule out live processing. They don't rule out inference. They don't rule out audio-derived signals that never exist as stored recordings.

Not recording doesn't mean not processing.
Not storing doesn't mean not analyzing.
Not using "conversations" doesn't mean not detecting context.
- https://medium.com/@giraldo_12272/our-devices-are-listening-to-us-64f79723e8f3

But simply placing your device in another room should be a sufficient precaution, though one should always carry out a test by making a voice recording while speaking on the next room, first. Some users report being able to turn targeted ad's off and on simply by disabling the WhatsApp microphone access on their phone. Worth experimenting with in a low risk scenario.

It is reasonable to be skeptical of companies such as Facebook who claim not to have used Active Listening for targeting ads, given their track record with selling users data as part of the Cambridge Analytica scandal. And their relationships with law enforcement. And political advertising. And their content moderators mental health. And their content moderation guidelines at all...

Further empirical clarity on this subject from a technical standpoint will be crucial going forward. However from a social and political perspective there is no ambiguity: private speech is central to the concept of free speech. And given the emphasis in this section on activists entering the public realm, as the political commentator and historian Hannah Arendt famously observed: there is no public space without private space. Here are some things you can do to at least prevent giving explicit permission to your tech to listen to you (whatever market they have found for the content): disable Siri across all iOS devices; don't allow microphone access to applications (this means individually disabling this feature manually for each app); disable "Hey Google" across android devices.

Password Managers

A credential spill, alternatively referred to as a data breach or leak, arises when unauthorized individuals or groups illicitly obtain access to sensitive user credentials that organizations store. Such credentials frequently comprise usernames, email addresses, and passwords. The repercussions of credential spills can be significant, as they commonly subject users to a range of hazards, including identity theft, financial fraud, and unauthorized account infiltration.

big tech ocean: publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**

Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts on other systems through large-scale automated login requests directed against a web application. Credential stuffing attacks are possible because many users reuse the same username/ password combination across multiple sites, with one survey reporting that 81% of users have reused a password across two or more sites and 25% of users use the same passwords across a majority of their accounts. In 2017, the FTC issued an advisory suggesting specific actions companies needed to take against credential stuffing, such as insisting on secure passwords and guarding against

attacks. According to former Google click fraud czar [lol, that title] Shuman Ghosemajumder, credential stuffing attacks have up to a 2% login success rate, meaning that one million stolen credentials can take over 20,000 accounts. Wired Magazine described the best way to protect against credential stuffing is to use unique passwords on accounts, such as those generated automatically by a password manager, enable two-factor authentication, and to have companies detect and stop credential stuffing attacks.
- Retrieved from Wikipedia 19.02.2025: https://en.wikipedia.org/wiki/Credential_stuffing

In order to keep track of many long, unique passwords (with different ones for phone, computer, every account, etc.), use a password manager. This allows you to use a single password to open the file that contains all of your passwords. Many password managers can also generate passwords and passphrases for you when you add an entry. Needless to say, the password for your password manager file must be strong and needs to stay secret! Memorize it as soon as possible. Though discouraged, if you absolutely need to keep a written hard copy, store it in a different location than the data it protects (and somewhere likely safe from police raids, seizure, or destruction). And make sure to keep backups of your password manager... or else you will be locked out of all your accounts. Suggested password managers: KeePassXC on desktop, AuthPass or KeePassDX on Android, 1Password on desktop and mobile for iOS, Android and Linux, on mobile for iOS and Android. It can however be tricky to make backups and sync password managers across devices.

Passwords

It is absolutely true that people make passwords hard to remember because they think they are "safer", and it is certainly true that length, all other things being equal, tends to make for very strong passwords. A password such as "Tr0ub4dor&3" is bad because it is easy for password cracking software and hard for humans to remember, leading to insecure practices like writing the password down on a post-it attached to the monitor. On the other hand, a password such as "correct horse battery staple" is hard for computers to guess due to having more entropy but quite easy for humans to remember. Extracted from: https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength

big tech ocean: publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**

Full Device Encryption

Encryption is complicated math equations that turn data from useful info into scrambled nonsense (and the opposite, decryption). Device encryption can be implimented via Bitlocker for Windows (but not on certain versions like Windows 10 and 11 Home Edition or older), LUKS for Linux (though this must be done at the point of set up), and Filevault on iOS. Each operating system is different, so follow the user guides provided by the company.

big tech ocean:
publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**

The purpose of device encryption is to prevent physical access - it does not address remote access to the device at all. For a phone, use a PIN of length 6 that is not used anywhere else and change it, if someone sees it over your shoulder. For computers use a long good password as described above. If your device is openable via biometrics, such as a fingerprint or your face, this is a weakness to be avoided and feature to be deactivated especially on protest days. Here are some scenarios that create the need for full device encryption. Remember most new smartphones are already encrypted by default, so the key to your security there is having a long unique (screenlock) password required to open it. Don't forget to update your software to protect against both in person and remote access. Only full device encryption on an up to date phone or computer provides protection against the extraction of, for example, Signal history from a seized device. In fact, modern android and iOS devices have a chip that handles decryption and pauses after a few wrong guesses. This is the main protection, an only works if encryption is enabled. If it is not, the PIN like cannot prevent police data extraction. If it is, then the chip is the main protection. Otherwise it only takes a few minutes to crack an eight digit pin.

When filming the authorities in situations of medium to high risk, ideally use the camera/microphone while the screen is locked, which is possible on many phone models and operating systems. This way if your device is rapidly seized, other features are not immediately available, provided that it has been fully encrypted.

CoMaps, powered by Open Street Maps

https://www.openstreetmap.org/

OpenStreetMap is built by a community of mappers that contribute and maintain data about roads, trails, cafés, railway stations, and much more, all over the world. It is an important, free, alternative to Google Maps given that Amnesty International have warned of Google's complicity in human rights violations, cooperating with repressive governmental regimes and their dropping of the pledge to not to use AI for weapons or surveillance. CoMaps is a free & open-source map/navigation app (mainly) for Android and iOS, that is based on OpenStreetMap data and focuses on a privacy-respecting, offline-map use. Users can download the map areas they need to their phone and then navigate those maps fully offline.

pond of autonomous tech infra:
riseup, autistici/inventati, systemli, etc

MISTY

data is minimized as a principle, identities remain anonymous

Wear a: **PAPER BOAT**

Using Cryptpad

https://cryptpad.cz/ is an end-to-end encrypted collaborative workspace. To use Crytpad it is crucial to create an account and start and share new documents from that account. Otherwise anyone with the link to the files you create can get access to them at any time in the future - including deleted content from the file! By making an account you are permitting yourself to retroactively go back and delete files you no longer want to have shared with specific individuals (or anyone who get hold of that link). When sharing the pad with others do not share the URL link in the browser bar, but rather be sire to hit "Share" and determine the level of access the link permits (much like a shared Google Document).

pond of autonomous tech infra:
riseup, autistici/ inventati, systemli, etc

MISTY

data is minimized as a principle, identities remain anonymous

Wear a: **PAPER BOAT**

* * *

Your boat has made it this far. Congrats. God only knows where you have landed up. You're still out sailing through rivers of data each day and the water feels strangely familiar yet completely different. Perhaps a new subtext lurks beneath the waves. It's time to plot a course for a safe harbor, lower sails and continue to get organized.

Browsing the Internet with TOR - The Onion Router

The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way. This is still a simple explanation for how Tor works today. https://www.torproject.org/about/history/ Do not access websites requiring login through Tor unless you have done lots of research on how to do this safely. Tor users may still be identifiable on phones or with Brave through "browser fingerprinting". For a reasonable degree of safety, do research for activism if you're using Tor, only on Tor Browser Bundle for Desktop/Laptop.

pond of autonomous tech infra:
riseup, autistici/inventati, systemli, etc

MISTY

data is minimized as a principle, identities remain anonymous

Wear a: **PAPER BOAT**

Mastodon

Mastodon is a free and open-source software platform for decentralized social networking with microblogging features. It operates as a federated network of independently managed servers that communicate using the ActivityPub protocol, allowing users to connect across different instances within the Fediverse. Each Mastodon instance establishes its own moderation policies and content guidelines, distinguishing it from centrally controlled social media platforms. Follow and Boost with gusto and always

write alt text for your images people. Two instances that are recommended rather than mastodon.social are Kolektiva.social - an anti-colonial anarchist collective that offers federated social media to anarchist collectives and individuals in the fediverse, whose users are based more in the United States, and the Todon.eu instance - a radical leftist anti-authoritarian Mastodon server. We welcome anarchists, socialists, (climate) activists, the LGBTQIA+ community, environmentalists, anti-racists, anti-fascists, anti-capitalists, intersectionalists, vegans, human rights activists, etc. As far as they are radical, leftist and anti-authoritarian. Good, free Mastodon apps for mobile are hard to come by but Tusky is recommended for Android

pond of autonomous tech infra:
riseup, autistici/inventati, systemli, etc

MISTY

data is minimized as a principle, identities remain anonymous

Wear a: **PAPER BOAT**

Social Media

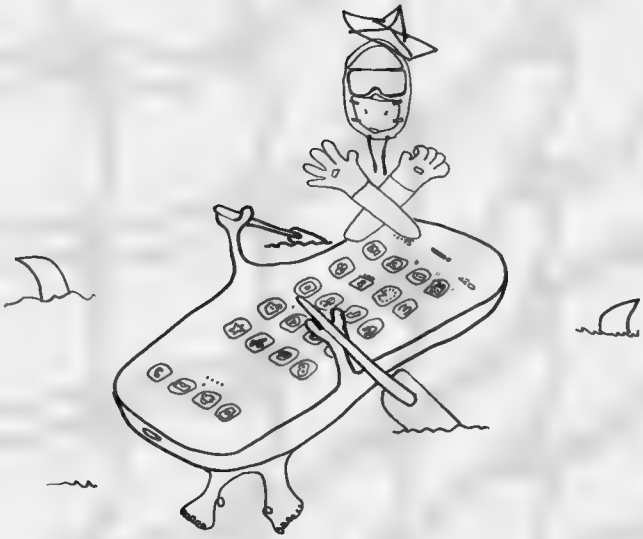
From a data faring security perspective, social media is viewed as a public record that users have no ability to control once they have agreed to post content there (this includes drafts, and so called direct or personal messages). Think about how the information you make public contributes to a wider data set about you. There are a variety of stances on this issue around self censorship and how to make informed decisions about your public profile. The subject is certainly worth another deep dive.

big tech ocean:
publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**



VPNs

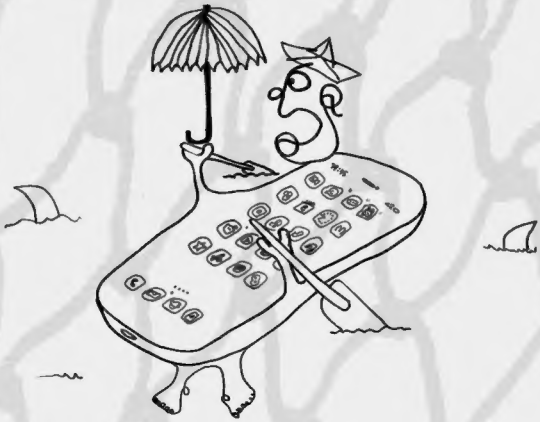
One last thing you might want to consider is adding a VPN to your data flow security measures. However, VPNs do two things and two things only: 1. Prevent your ISP from getting the logs of which servers you are connected to, and the contents of unencrypted traffic (the later of which is increasingly rare for many sites) and 2. Prevent services you connect to from knowing your IP. (On cell networks this information is not especially identifying.) It does absolutely nothing to prevent the vast majority of identity correlations, fingerprinting and behavioral analysis. Or the continued data transmission via authenticated apps (where the user is signed in as themselves) and provides a false sense of security in most use cases. VPNs can be a way to improve your privacy but incur costs, are difficult to set up and face performance degradation.

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**



The Potential Threat of 'AI' or Large Language Models (LLM's) to Privacy and Security

big tech ocean:

publicly traded, monopolistic - google, meta, etc)

ROUGH WEATHER

demands enhanced protection and planning

You will need: **FACE MASK, GLOVES and GOGGLES**

Artificial intelligence reduces the human labor and therefore cost required to analyze large datasets in a way that impacts privacy. This means that large datasets which previously could be trawled through to find data about an individual can soon be systematically analysed to extract actionable information about large numbers of individuals, or determine which individuals to target, more effectively than before. Law enforcement advocates have tried to ban end-to-end encryption for years, but civil society has pushed back mostly successfully. However, end-to-end encryption does not protect messages from being read by the end device itself. The new practice of training or testing AI on the contents of such messages - called clientside scanning - may permanently undermine end-to-end encryption platforms. WhatsApp has recently introduced a tool that is opt-in for now, for that specific application. Windows has introduced a feature called "Recall" that takes screenshots of whatever is onscreen for AI training that is also opt-in for now. However, Signal developers quickly opted the Signal Desktop application out of Recall screenshots so that it will not be affected - however, few other companies will be inclined to do this as data mining for 'AI' has become the digital marketing choice of the day. Window's users, please be on the lookout for pop-up windows of the system prompting you to opt into activating Recall / Copilot+. Microsoft will download the software automatically, but they will not turn on unless you agree, so it's absolutely crucial to not opt-in. If you want to make sure you haven't opted in accidentally, try going to Settings > Privacy & Security > Recall & Snapshots and turn off "Save snapshots" if it on. Also be sure to delete any existing snapshots. USE: https://noai.duckduckgo.com to filter out the noise.

Browsers

As mentioned above under Apps, web browsers vary in strength with regards to privacy and security. Vivaldi, Firefox, Brave and Chrome without Google login are a better choice than Safari though the integration as standard of 'Ai' or large language models into companies such as Mozilla Firefox and Duck Duck Go have drawn criticism from privacy advocates. ~~Vivaldi is also fast, customizable, privacy focussed, mental-health friendly browser (it has a pause button for the app), without forced 'AI' integration.~~

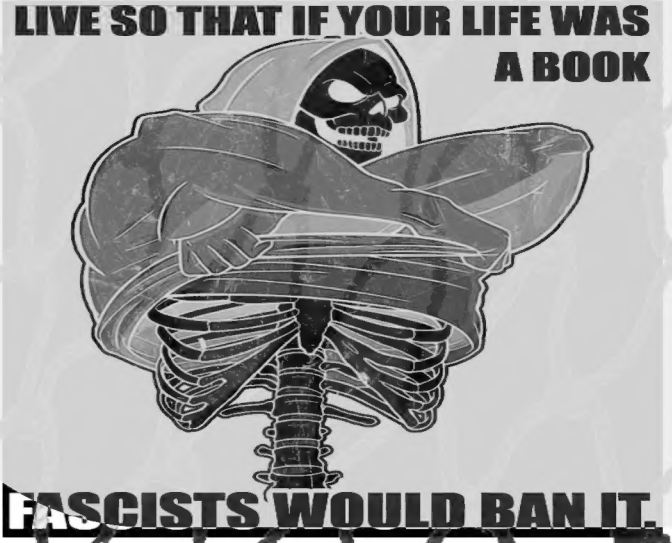
However, the settings used in a web browser are more important than the choice of browser, except in the case of targeted attacks.

private company river:
private companies (proton, mullvad, posteo, etc)

UNPREDICTABLE WEATHER

prepare for future changes in ownership

Take: **UMBRELLA**



Index:

Hard Borders 26

Using Signal 33

Not Using Telegram 36

Email 36-37

Apps 38

Not Sharing PDFs 39

Tracking & Social Network Mapping 41

Active Listening 44

Password Managers 47

Passwords 50

Full Device Encryption 50-51

CoMaps, powered by Open Street Maps 52

Using Cryptpad 53

Browsing the Internet with TOR 54

Mastodon 54-55

Social Media 56

VPNs 57

‘AI’ or Large Language Models (LLMs) 58

Browsers 59